



Treasury Inspector General for Tax Administration

SUFFICIENT EMPHASIS WAS NOT PLACED ON RESOLVING SECURITY VULNERABILITIES WHEN RESTORING THE ELECTRONIC FRAUD DETECTION SYSTEM

Issued on June 14, 2007

Highlights

Highlights of Report Number: 2007-20-108 to the Internal Revenue Service Chief, Criminal Investigation; Chief Information Officer; and Chief, Mission Assurance and Security Services.

IMPACT ON TAXPAYERS

The Electronic Fraud Detection System (EFDS) is used by the Internal Revenue Service (IRS) Criminal Investigation Division to detect fraudulent returns and to prevent the issuance of questionable refunds. The EFDS is the IRS' second largest repository of taxpayer data. Security over the System is vital to ensure it is available to prevent fraud and to protect the privacy of taxpayers' personal information.

WHY TIGTA DID THE AUDIT

This audit was initiated to follow up on a prior TIGTA audit. In September 2006, TIGTA reported that the security of the EFDS had not been properly assessed since 2001, and recommended the Chief, Mission Assurance and Security Services, in coordination with the Chief, Criminal Investigation, complete a security certification and accreditation for the EFDS and supporting computers before the restored EFDS was permitted to operate. The overall objective of this audit was to assess the effectiveness of the security controls testing conducted as part of the certification and accreditation of the EFDS.

WHAT TIGTA FOUND

The EFDS security controls were effectively tested and evaluated. However, the Criminal Investigation Division and the EFDS Project Office missed an opportunity to correct some of the significant security vulnerabilities prior to restoring the EFDS in January 2007.

The Chief, Criminal Investigation, granted a "restricted authorization to operate" for the EFDS. This is not a valid accreditation decision. An Interim Authorization to Operate, rendered when vulnerabilities are significant but can be addressed

timely, would have been the appropriate accreditation decision for the EFDS.

WHAT TIGTA RECOMMENDED

TIGTA recommended the Chief, Criminal Investigation, issue an Interim Authorization to Operate for the EFDS and require specific terms and conditions be met before an Authorization to Operate is granted.

In their response to the report, IRS management disagreed with the recommendation. The Chief, Mission Assurance and Security Services, stated that the decision of the Chief, Criminal Investigation, to issue an Authorization to Operate is fully supported because (1) no "high" security risks were identified for the EFDS and (2) an updated Plan of Action and Milestones is in place and being maintained to address issues identified during the certification that have not yet been resolved.

TIGTA does not agree with IRS management's response to the recommendation. Federal Government security standards state that an Interim Authorization to Operate is appropriate when weaknesses are significant but can be corrected timely. The IRS' certification of the EFDS identified weaknesses TIGTA considers to be significant because they increase the risk that unauthorized accesses could be made to the EFDS without detection. TIGTA recognizes the accreditation decision is subjective but believes issuance of an Interim Authorization to Operate is the more prudent accreditation decision for the EFDS because it would bring increased attention to resolving the significant security weaknesses of this important system.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full IRS response, go to:

<http://www.treas.gov/tigta/auditreports/2007reports/200720108fr.pdf>

Email Address: Bonnie.Heald@tigta.treas.gov
Web Site: <http://www.tigta.gov>

Phone Number: 202-927-7037